CODEC NET

Security Operations Center

On-demand Report

Global Finance Corp

Executive Summary

Report Period: November 27, 2025 - December 4, 2025

Top 10 Security Alerts

#	Severity	Alert Description	Host/Agent	Count	Last Seen
1	Major	Possible kernel level rootkit	wazuh-VMware-Virtual-Platform	3	12/02/25 10:59 AM

Alert Statistics & Trends

Alert Distribution

Critical	0
Major	3
Minor	0
Total Alerts	3

Alert Severity Breakdown

Critical: ▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓ 0

Major: ████████████████ 3

Minor: ▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓ 0

Critical: 0% | Major: 100% | Minor: 0%

Daily Alert Trend (Last 7 Days)

Tue, 12/2: ████████████████████ 3

Top 5 Alert Types

ossec	3

Agent Status Overview

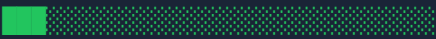## Agent Summary

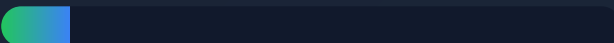|	
Total Agents	**9**
Active	**1**
Disconnected	**8**
Never Connected	**0**

Agent Health Status

Active: **1**

Disconnected: **8**

Never Connected: **0**

OVERALL HEALTH

11%

Agent Details

wazuh-VMware-Virtual-Platform — **Active**

OS: Ubuntu
IP: 127.0.0.1
Version: Wazuh v4.13.1
Last Seen: 1/1/10000, 5:29:59 AM

windows — **Disconnected**

OS: Microsoft Windows 11 Home Single Language
IP: 192.168.1.5
Version: Wazuh v4.13.1
Last Seen: 9/26/2025, 5:56:58 PM

Ubuntu_yara — **Disconnected**

OS: Ubuntu
IP: 192.168.1.29
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 1:20:48 PM

Centos_yara — **Disconnected**

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 2:27:33 PM

localhost.localdomain — **Disconnected**

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 4:43:08 PM

YARA_NEW — **Disconnected**

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 4:50:07 PM

Yara_Final　Disconnected

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 5:12:54 PM
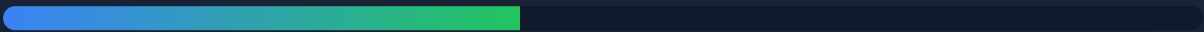
Yara_New_2.0　Disconnected

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 5:44:07 PM

Overall Compliance Score   43%

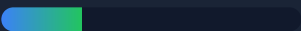## Security Configuration Assessment - Per Policy

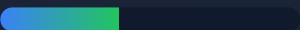CIS CentOS Linux 9 Benchmark (515 passed, 490 failed)
51%

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 (127 passed, 349 failed)
27%

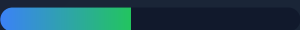CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0. (96 passed, 149 failed)
39%

CIS Distribution Independent Linux Benchmark v2.0.0. (83 passed, 99 failed)
46%

CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0. (76 passed, 101 failed)
43%

Agent Compliance Scores

1. Yara_New_2.0
103 passed, 98 failed (1 policies)
51%

2. Centos_yara
103 passed, 98 failed (1 policies)
51%

3. localhost.localdomain
51%

4. YARA_NEW
103 passed, 98 failed (1 policies)

51%

5. Yara_Final
103 passed, 98 failed (1 policies)

51%

6. Sunny_Windows
83 passed, 99 failed (1 policies)

46%

7. Ubuntu_yara
76 passed, 101 failed (1 policies)

43%

8. wazuh-VMware-Virtual-Platform
96 passed, 149 failed (1 policies)

39%

9. windows
127 passed, 349 failed (1 policies)

27%

Configuration Findings Summary

Total Checks	**2085**
Passed	**897**
Failed	**1188**

Overview

During the reporting period of November 27, 2025 - December 4, 2025, our Security Operations Center monitored and analyzed 3 security alerts across your infrastructure. The alert distribution shows 0 critical alerts, 3 major alerts, and 0 minor alerts.

Our team has been actively monitoring, triaging, and responding to security events in real-time. 9 agents are deployed across your infrastructure, with 1 currently active.

Security configuration assessment shows an overall compliance score of 43% with 1188 failed checks requiring attention.